Hacia un marco europeo sobre firmas digitales y criptografia

Vinje, Thomas; Julia, Rosa

Published in:
Revista de Derecho Mercantil

Publication date:
1998

Document Version
le PDF de l'éditeur

Hacia un marco europeo sobre firmas digitales y criptografía

La Comisión Europea da un paso adelante en pro de la confidencialidad y seguridad en las comunicaciones electrónicas

POR

ROSA JULIÀ BARCELÓ Y THOMAS VINJE (1)

SUMARIO: I. Introducción: aspectos tecnológicos: *Criptografía*; *Firmas digitales y su infraestructura; El papel de las autoridades de certificación*.—II. Establecimiento de un marco legal para las autoridades de certificación: *¿Cómo conseguir un amplio reconocimiento y generación de confianza en los certificados digitales?; ¿Debería este marco legal basarse en un sistema de licencias, sin licencias, o un sistema que permita ambos?; ¿Qué régimen de responsabilidad debería aplicarse?*—III. Reconocimiento legal de las firmas digitales.—IV. Regulación de la criptografía: *Medidas de control de la exportación; Medidas de control doméstico; Sistemas de Key escrow y key recovery; Intimidad; Tendencias legislativas de la Comisión*.—V. Conclusión.

El crecimiento del comercio electrónico depende de la capacidad de los mensajes electrónicos para ser confidenciales y seguros. La necesidad de confidencialidad y de seguridad se encuentra en varios tipos de comunicaciones electrónicas, en las que cabe incluir, por ejemplo, contratos electrónicos (entre comerciantes, entre comerciantes y consumidores), declaraciones de impuestos por medios electrónicos, historiales clínicos. Como se describe más abajo, hoy en día, la principal herramienta técnica para asegurar la confidencialidad y seguridad de las comunicaciones electrónicas es la infraestructura de firma digital y la criptografía.

El 8 de octubre de 1997, la Comisión Europea dio un paso adelante hacia el establecimiento de un marco Europeo sobre la firma digital y la criptografía a través de la aprobación de una Comunicación titulada "Asegurando un marco legal sobre firmas digitales y criptografía. Hacia un

(1) Thomas Vinje es abogado y socio del despacho norteamericano Morrison & Foerster (oficina de Bruselas). Rosa Julià Barceló es profesora ayudante de Derecho mercantil de la Universidad de las Islas Baleares y colaboradora con el "Centre de Recherches d'Informatique et Droit" en Namur, Bélgica.

marco Europeo sobre firmas digitales y criptografía" (2-3). La Comunicación se divide en tres secciones. La primera trata de la elaboración de un marco que gobierne las entidades que emitirán los certificados estableciendo con ello una base para la firmas digitales (las llamadas autoridades de certificación), así como el reconocimiento legal de las firmas digitales. El segundo se centra en la criptografía con fines de obtener la confidencialidad de las comunicaciones, incluyendo medidas para el control de la exportación y requisitos para hacer cumplir la ley. Por último, la Comunicación trata las bases legales para emprender una iniciativa comunitaria en estas materias, su conveniencia y el plazo temporal para llevarlo a cabo.

Este artículo, después de ofrecer una introducción tecnológica sobre la que se basa la Comunicación, tiene como objetivo describir y analizar los aspectos principales tratados por la Comunicación, incidiendo especialmente en la cuestión de las firmas digitales y las autoridades de certificación.

I. Introducción: aspectos tecnológicos

Tanto las firmas digitales como la criptografía a los fines de lograr confidencialidad se basan en técnicas criptográficas. En efecto, una firma digital es esencialmente un mensaje encriptado o codificado que acompaña un mensaje electrónico. Sin embargo, como se describe más adelante, las firmas digitales y la criptografía para confidencialidad tienen funciones diferentes y normalmente están basados en técnicas criptograficas distintas.

Criptografía

Tal y como se usa en la Comunicación, criptografía es el término que se utiliza para describir los criptosistemas simétricos o de clave privada cuya función es conseguir la confidencialidad de las comunicaciones electrónicas. La utilización de criptografía simétrica en las comunicaciones electrónicas tiene la función de encriptar o codificar la comunicación de modo que únicamente las partes de dicha comunicación, es decir, el originador y el destinatario, puedan leer el contenido de la misma.

La utilización del sistema de criptografía simétrica o de clave privada requiere que el emisor y el receptor utilicen la misma clave para encriptar y desencriptar los mensajes: el emisor encripta el mensaje con la clave pri-

(2) La traducción de la Comunicación es del autor al no existir versión oficial en español.

(3) Com. (97) 503 (De aquí en adelante Comunicación). Esta Comunicación fue prevista en abril de 1997 por la Comunicación de la Comisión titulada "Una Iniciativa Europea en Comercio electrónico", COM (97), 157 final, 14-4-97. La Dirección General XIII de la Comisión redactó un "Libro Verde" sobre el mismo tema, terminado el 24 de abril de 1994, titulado *Libro verde sobre seguridad de los sistemas de información*, el cual no fue publicado oficialmente.

vada y lo envía al receptor, quien aplicando la misma clave al mensaje encriptado lo desencriptará (es decir, lo pasará de texto codificado a texto claro o legible, devolviéndolo a su forma original). Para que dichas comunicaciones sean verdaderamente confidenciales, la clave compartida debe ser guardada en secreto.

A pesar de que la Comunicación utiliza el término criptografía para describir sólo sistemas de clave simétrica o privada, también es posible utilizar, tal y como se describe más abajo, sistemas criptográficos de clave pública para conseguir la confidencialidad en las comunicaciones.

Firmas digitales y su infraestructura

Mientras la criptografía tal y como se emplea en la Comunicación es utilizada para conseguir la confidencialidad de las comunicaciones, la tecnología de la firma digital tiene como objetivo lograr la autenticidad e integridad de los mensajes de datos, esto es, la seguridad de las comunicaciones electrónicas. Por medio del uso de la firma digital y su infraestructura, el receptor de una comunicación electrónica puede tener la seguridad que el emisor de la comunicación es la persona que pretende ser, lo cual es normalmente conocido como función autentificadora de la firma digital. Además, el receptor del mensaje puede también tener la seguridad que el mensaje recibido es el mismo que fue enviado, es decir, que no ha sido alterado durante la transmisión del mismo, característica ésta denominada función de integridad.

La firma digital y su infraestructura está basada en criptografía de clave publica o asimétrica en la que se utilizan dos claves diferentes pero matemáticamente relacionadas entre sí, una para encriptar los mensajes y otra para desencriptarlos. En un sistema de criptografía de clave pública, cada parte deberá tener dos claves diferentes. Una clave es utilizada para transformar los datos en una forma aparentemente ininteligible. Dichos datos se adjuntan al documento electrónico (que puede estar en claro o encriptado) y constituyen la firma digital en sí misma. La otra clave es utilizada para verificar la firma digital, es decir, devolver el mensaje que constituye la firma digital a su forma original. En otras palabras, el emisor de un mensaje electrónico lo firma digitalmente por medio de la inclusión de ciertos datos encriptados utilizando una clave (de la misma manera que el autor de un documento tradicional firma por medio de la inclusión de su firma manuscrita al documento mismo). El receptor del documento electrónico verifica la validez de la firma digital desencriptando el mensaje por medio de la utilización de la otra clave.

La clave utilizada para crear la firma digital, la clave para firmar, se llama clave privada porque es utilizada únicamente por el firmante. A menos que esta clave haya sido robada o de otra manera puesta en peligro, nadie más tiene acceso a esta clave y, consecuentemente nadie más puede firmar digitalmente el mensaje de la misma manera.

La segunda clave, esto es, aquella utilizada para verificar la firma, se llama clave pública debido a que de ordinario es conocida por mas perso-

nas (es accesible al publico en general), por ejemplo mediante un directorio de claves públicas. Cuando la clave pública se aplica a la firma digital creada con la clave privada matemáticamente relacionada con la pública, el poseedor de la clave pública desencriptará esta firma y sólo esta. En consecuencia, la clave pública no reconocerá, esto es, no podrá verificar, la firma digital de otra persona.

Debido a que una clave pública sólo puede verificar la firma digital que ha sido creada con la clave privada matemáticamente relacionada con dicha clave pública y como el emisor de un mensaje es el único poseedor de la clave privada (siempre que no haya sido descubierta, robada o puesta en peligro de otra manera), el receptor de un mensaje acompañado de una firma digital la cual es verificada con éxito por medio de la aplicación de la clave pública del emisor, puede tener la confianza que el mensaje es auténtico, esto es, que fue enviado por la persona que dice ser la emisora. Además, después de aplicar la clave pública al mensaje encriptado o firmado, el receptor puede comparar el texto resultante al texto en claro incluido en el mensaje. Si son idénticos, el receptor puede tener confianza de la integridad del mensaje, es decir, que el mensaje no ha sido modificado durante la transmisión electrónica del mensaje.

En la mayoría de sistemas de criptografía de clave pública se aplica un algoritmo unidireccional al mensaje (conocido habitualmente como función de "hash") dando como resultado una versión comprimida o reducida del mismo mensaje. La versión comprimida del mensaje (conocido como "message digest") es la que posteriormente será firmada con la clave privada del emisor del mensaje. Así pues, dicha versión comprimida y firmada del mensaje es lo que constituye propiamente la firma digital.

Debido a que el algoritmo es unidireccional, el resultado o versión condensada no puede volverse hacia atrás para lograr la versión no comprimida del mensaje. En consecuencia, la versión comprimida del mensaje y firmada con la clave privada se adhiere al mensaje completo y en claro (opcionalmente y por motivos de confidencialidad puede encriptarse). El receptor, una vez recibido el mensaje y tras haber verificado la firma por medio de la aplicación de la clave pública del emisor, aplicará al mensaje en claro el mismo algoritmo unidireccional que aplicó el emisor (es decir, la más arriba llamada función de "hash"), y comparará el resultado con el mensaje previamente verificado. Si el mensaje cuya firma se ha verificado fue objeto de alteración durante la transmisión del mismo, las dos versiones comprimidas serán diferentes, revelando que el mensaje ha sido modificado (4).

En relación a la autoría del mensaje, el receptor puede confiar en la identidad del emisor sólo si tiene la seguridad que la clave privada permanece en posesión de la persona con la que cree estar comunicando y que esta parte, con la cual está comunicando, es realmente la que pretende ser. En consecuencia, el sistema de claves debe permitir al receptor de una comunicación electrónica tener la seguridad que la clave privada del emi-

(4) Ver US. Congress, Office of Technology Assessment, Issue Update on Information Security and Privacy in Network Environments, Washington, D. C., 1995, pág. 49.

sor no ha sido robada, copiada o de cualquier otra forma puesta en peligro. Por ejemplo, el sistema debe permitir a una parte comunicante como sería un farmacéutico, ante la recepción de una receta emitida por un médico, comprobar si la clave privada del mismo ha sido robada o puesta en peligro de otra forma antes vender las medicinas. Dicho sistema también debería permitir al receptor del mensaje electrónico, no sólo asegurarse de que la parte con la que el receptor está comunicando es la que realmente dice ser, sino también si tiene las características que el emisor pretende tener. Siguiendo con el anterior ejemplo, el farmacéutico debería poder asegurarse que el poseedor de tal clave pública que corresponde con tal clave privada es realmente un medico antes de aceptar la receta médica. Tal y como se describe más abajo, ambos objetivos pueden ser conseguidos a través de las actividades llevadas a cabo por las autoridades de certificación.

Es corriente incluir la clave pública juntamente con el mensaje electrónico. Sin embargo, a través de dicho recurso, el receptor no puede tener la seguridad necesaria sobre la integridad de la clave privada, (esto es, que no ha sido robada, copiada o de otra manera comprometida). A pesar de que un receptor puede utilizar la clave pública que se acompaña al mensaje firmado para verificar la firma, la única forma para adquirir plena certeza sobre la integridad de la firma digital es a través de la obtención de la clave pública de un directorio de claves plenamente fiable y seguro. El hecho de incluir la clave pública junto al mensaje firmado y que la misma pueda ser utilizada para verificar el mensaje, no indica necesariamente que la clave privada continúe en la sola posesión del verdadero y originario detentador de la clave privada.

Como se describe más abajo, lo anterior subraya una de las funciones más importantes de las autoridades de certificación: el establecimiento y mantenimiento de una base de datos en la que se contendrían las claves públicas. A través de la emisión de certificados a los poseedores de las claves y creación y mantenimiento de la base de datos, las autoridades de certificación juegan un papel esencial en el establecimiento de un sistema seguro en el que los receptores de mensajes pueden verificar la integridad de las claves, así como las características de los titulares de las mismas.

En consecuencia, la firma digital ofrece la misma función que la firma manuscrita, es decir, ofrece integridad y autenticidad. Así pues, la firma digital, acompañada un sistema de claves públicas y privadas estructurado y gestionado de manera adecuada, aplicando algoritmos seguros y con claves suficientemente largas, es virtualmente imposible de falsificar pudiéndose afirmar que ofrece más fiabilidad que la firma manual (5). En consecuencia, un sistema de comercio electrónico basado en documentos electrónicos y firmas digitales tiene la potencialidad de ofrecer más seguridad que nunca.

(5) La capacidad para descubir la clave privada a partir de la clave pública aumenta a medida que la tecnología y poder de computación progresa. En consecuencia, la longitud necesaria de la clave para obtener una firma digital fiable debería ser constantemente revisada así como la seguridad de los algoritmos. Lo que es más, la tecnología debe asegurar también la seguridad de la red. La administración de las claves debe llevarse a cabo en un entorno seguro.

Como se dijo más arriba, un sistema de criptografía asimétrica puede ser usado no solo para conseguir autenticidad e integridad a través de la firma digital y autoridades de certificación, sino también confidencialidad de las comunicaciones. En efecto, los mensajes electrónicos a los que se adhiere una firma digital a menudo son encriptados con la clave pública del receptor. En consecuencia, sólo el receptor con la utilización de su clave privada podrá desencriptar el mensaje.

El papel de las autoridades de certificación

Como se dijo más arriba, la seguridad de las firmas digitales y, en consecuencia, su valor en el comercio electrónico se basa fundamentalmente en la fiabilidad de las claves. En un marco de redes abiertas, el requisito de fiabilidad de las claves puede conseguirse sobre todo a través de un régimen legal que rija autoridades de certificación independientes, las cuales proporcionarán: (I) la garantía necesaria sobre la identidad del emisor de un mensaje a través de la emisión de certificados que liguen las claves públicas con la identidad de sus poseedores; (II) la seguridad que las claves no han sido robadas o de otra manera puestas en peligro a través del establecimiento de una base de datos fiable y el mantenimiento al día de las claves que permanecen válidas (6).

Para ofrecer la confianza entre las partes comunicantes sobre la identidad y las características de los poseedores de claves, la autoridad de certificación debe obtener y verificar ciertas informaciones del solicitante de un certificado. Por ejemplo, un médico que solicita un certificado debe ofrecer una demostración adecuada de su identidad personal y de su habilitación para ejercer la medicina. Después de obtener y verificar dicha información, la autoridad de certificación crea un certificado que incluirá, entre otros aspectos, la clave pública del solicitante del certificado (7), la identidad del solicitante del certificado, un número de serie y la identidad de la autoridad de certificación. Entonces, se aplica una función de "hash" dando como resultado un mensaje comprimido que será firmado por la autoridad de certificación con su clave privada. Esta firma es adherida a la misma información en claro, lo cual formará el certificado digital. Así pues, el certificado tendrá dos partes: la parte no encriptada o en claro y la parte que contendrá la firma digital de la autoridad de certificación.

(6) En el pasado, la mayoría de publicaciones utilizaban la expresión terceros de confianza —trusted third parties— para refererise tanto tanto las autoridades de certificación como a los actores que llevaban a cabo las funciones de *key escrow* y *key recovery*. Sin embargo, la Comunicación, siguiendo las OECD Guidelines for Cryptography Policy (29 marzo de 1997), utiliza la palabra autoridades de certificación para aquellas actividades que llevan a cabo servicios de autenticación y usa el término "*trusteed third party*" exclusivamente para referirse a aquellos sujetos que llevan a cabo servicios relativos al acceso legal a las llaves privadas o para encriptar (*key escrow and key recovery*).

(7) Normalmente, el solicitante de un certificado genera su propio par de claves (privada y pública) y entrega la clave pública a la autoridad de certificación cuando solicita el certificado.

Este certificado permite a las partes comunicantes tener la seguridad sobre la identidad y las características de las partes con las cuales están comunicando de la manera que se describe a continuación: cuando A envía a B un mensaje firmado también envía junto al mensaje el certificado emitido por la autoridad de certificación, y debido a que la clave pública de la autoridad de certificación es pública y fácilmemente accesible en una base de datos, B puede usar la clave pública de la autoridad de certificación para verificar la firma del certificado enviado por A con el mensaje, el cual contiene la clave pública de A.

Como se indicó más arriba, la segunda función principal de las autoridades de certificación es proporcionar certidumbre de que las claves continúan siendo válidas. Para conseguirlo, debe establecerse una base de datos publica en la que se incluya un lista de los certificados revocados. Esta lista debe indicar los certificados que no son válidos porque, por ejemplo, la clave privada ha sido robada, copiada o puesta en peligro de alguna otra manera. En consecuencia, cuando alguien reciba una mensaje electrónico que pretenda estar fimado por una persona determinada, el receptor puede confirmar que el certificado continua siendo válido a través de la comprobación en la lista de certificados revocados si dicho certificado está incluido en la lista de certificados revocados o si continua siendo válido.

II. Establecimiento de un marco legal para las autoridades de certificación

En la actualidad, los servicios de autoridad de certificación son ofrecidos en Europa por algunas compañías privadas especializadas en seguridad informática, cuyo establecimiento y operación no está sujeta a ningún marco legal (8). Debido a que las autoridades de certificación tendrán un papel vital en el establecimiento de un sistema fiable de comercio electrónico basado en la tecnología de la firma digital, el crecimiento de este sector dependerá de la adopción de un régimen legal adecuado, no excesivamente burocrático, que genere confianza en las actividades de las autoridades de certificación.

En la medida en que el régimen legal engendre más confianza en las autoridades de certificación y en el uso de las firmas digitales, por ejemplo ofreciendo más seguridad en el valor de los documentos electrónicos acompañados por certificados digitales, estimulará el comercio en general. Es más, el comercio electrónico transfronterizo solo florecerá si los certificados emitidos en un Estado Miembro son reconocidos en los demás Estados Miembros, y si el régimen legal que gobierna las autoridades de certificación está razonablemente armonizado.

El establecimiento de un régimen legal adecuado que gobierne el establecimiento y funcionamiento de las autoridades de certificación tendría

(8) Por ejemplo, en Bélgica la compañía Isabel ofrece los servicios de certificación en el sector bancario y Belsign los ofrece al gran público.

otras consecuencias favorables: podría poner las bases para el crecimiento del comercio electrónico en un contexto global, más allá de las fronteras de Europa, y ofrecer adecuada protección al consumidor en el contexto de los servicios de certificación.

La Comisión se plantea tres cuestiones pertinentes respecto de las autoridades de certificación:

— ¿Cómo se puede establecer un amplio reconocimiento legal en la Unión Europea, así como generar confianza en los certificados digitales?

— El marco legal que gobierne el establecimiento de las autoridades de certificación y su funcionamiento, ¿debería ser establecido a través de un sistema de licencias, un sistema sin licencias o la coexistencia de ambos?

— ¿Qué tipo de responsabilidad debiera regir para las actividades de las autoridades de certificación?

¿Cómo conseguir un amplio reconocimiento y generación de confianza en los certificados digitales?

La Comunicación sugiere que el establecimiento de un amplio marco legal comunitario en el que se estipulen ciertos requisitos básicos para el establecimiento y funcionamiento de las autoridades de certificación ofrecería las bases para el reconocimiento mutuo de los certificados entre los Estados Miembros. En otras palabras, una vez que este marco legal haya sido establecido, un certificado emitido en un Estado Miembro debería ser reconocido en los demás Estados Miembros. La Comunicación ofrece algunos ejemplos de algunos aspectos respecto de los que podrían especificarse requisitos comunes, incluyendose, entre otros:

— seguridad de las autoridades de certificación y cumplimiento con las leyes de protección de datos personales;

— identificación fiable de los suscriptores de certificados (para asegurar que los suscriptores son identificados adecuadamente);

— cobertura mínima de seguro (para cubrir aquellos casos en los cuales la autoridad de certificación es responsable, por ejemplo, por haber identificado mal al suscriptor de un certificado);

— obligaciones técnicas (por ejemplo, asegurar que la clave privada y pública empleadas por el suscriptor de un certificado son fiables y que los algoritmos utilizados son adecuados);

— cualificación y seguridad del personal empleado por la autoridad de certificación.

En principio, parece que las áreas identificadas por la Comunicación para su inclusión en un posible instrumento legislativo Comunitario que gobierne las autoridades de certificación son en general materias adecua-

das para ser incluidas en semejante legislación —aunque sería bueno tener en cuenta la conveniencia de incluir una provisión que promoviera la interoperabilidad entre las autoridades de certificación—. Es más, el objetivo de crear un régimen armonizado en el que se fijen los criterios mínimos para el establecimiento y funcionamiento de las autoridades de certificación y la aplicación en general del principio de reconocimiento mutuo de los certificados emitidos por autoridades de certificación que cumplan con dicho régimen es una iniciativa loable. Ademas, la Comunicación parece sugerir la creación de un régimen lo suficientemente flexible que dejará lugar a la experimentación en esta nueva área, evitando la creación de obligaciones burocráticas demasiado pesadas.

¿Debería este marco legal basarse en un sistema de licencias, sin licencias, en un sistema que permitiera ambos?

Una de las cuestiones claves que debe resolverse en relación a la creación de un régimen armonizado para el establecimiento y funcionamiento de las autoridades de certificación es si las autoridades de certificación deberían obtener una licencia si un Estado Miembro, que hubiera establecido la obligación de obtener una licencia debería aceptar un certificado emitido por una autoridad de certificación sin haber obtenido licencia por estar en un Estado Miembro cuya legislación no contemplase tal obligación para establecerse y funcionar como autoridad de certificación. Como indica la Comunicación, actualmente algunos Estados Miembros están en vías de introducir sistemas voluntarios para el establecimiento y operación de las autoridades de certificación, mientras que otros consideran sistemas de licencia obligatoria para que las autoridades de certificación y firmas digitales sean capaces de ofrecer confianza (9).

La Comunicación admite que un sistema de licencias podría ser apropiado. Sin embargo, la Comunicación también reconoce la posibilidad de sistemas sin licencia. Efectivamente, la Comunicación dice "Licenciar es sólo uno de los métodos posibles que los Estados Miembros pueden aplicar para fomentar la confianza, reforzar la seguridad y promover el uso de firmas digitales válidas y legales. Organizaciones sin licencia pero altamente consideradas, sean públicas o privadas, podrían también ser consideradas tan fiables como autoridades de certificación".

En consecuencia, la Comunicación concluye que el régimen de la Unión Europea que gobierne las autoridades de certificación debería permitir "la coexistencia de autoridades de certificación licenciadas y no licenciadas". No se precisa con claridad lo que dicha coexistiencia llevará consigo, pero, en principio parece que un Estado Miembro con un sistema de licencias debiera aceptar certificados emitidos por autoridades de certificación sin licencia creadas según la legislación de aquellos Estados Miembros cuya legislación no establezca un sistema de licencia. Sin embargo, las autorida-

(9) Ver (A/CN.9/437) y (A/CN.9/WG.IV/wp.71). Ver también: MAUTH, R., *Digital Signatures to Power E-Commerce*, Byte, núm. 1, 1998, págs. 5-10.

des de certificación de los Estados Miembros, cualquiera que sea el tipo de autoridad (licenciada o no licenciada), debieran respetar y cumplir unos criterios mínimos regidores del establecimiento y funcionamiento de las autoridades de certificación previstas por la legislación de dicho Estado Miembro.

La opción de la coexistencia propuesta por la Comisión es una decisión inteligente. Dada la novedad y estado infantil de este tipo de negocio, debiera dejarse espacio para la experimentación. Por ejemplo, podría ser apropiado, en lo que concierne a las licencias de las autoridades de certificación, limitar las obligaciones de licencia sólo a aquellas autoridades de certificación que ofrecen los servicios al gran público (como se ha sugerido por el Reino Unido) y excepcionar a los grupos cerrados. La finalidad fundamental debería ser establecer un equilibrio adecuado que permita imponer obligaciones para el establecimiento y funcionamiento de las autoridades de certificación, suficientes para engendrar confianza en el uso de la tecnología de la firma digital sin que con ello se coarte la recién nacida práctica negocial y tecnología de la certificación.

¿Qué régimen de responsabilidad debería aplicarse?

La Comunicación dice correctamente que "la tenencia de unas reglas de responsabilidad correctas contribuiría a la aceptación de los servicios de las autoridades de certificación". Sin embargo, la Comunicación no define claramente el criterio de responsabilidad. Al tratar la cuestión de responsabilidad, deberíamos distinguir claramente entre los siguientes actores: [1] el titular de un certificado; [2] la autoridad de certificación; y [3] la tercera parte receptora del certificado y que confía en él.

En relación a la potencial responsabilidad del titular de un certificado, que posiblemente tendrá una relación contractual con la autoridad de certificación, la letra de la Comunicación parece indicar que la responsabilidad de la autoridad de certificación dependerá de los términos del contrato. La Comunicación continua indicando que un "catálogo" de requisitos podría constituir la base para los deberes contractuales, previendo un mínimo y un máximo de responsabilidad a la que podría incurrir la autoridad de certificación. Sin embargo, la Comunicación no indica cuáles serán los requisitos que podría contener este catálogo ni tampoco si el contrato deberá incluir obligatoriamente dicho catálogo, ni tampoco si el régimen legal que gobierna las autoridades de certificación prohibirá la exclusión de responsabilidad en ciertas circunstancias, quizás para la protección del consumidor. Por ejemplo, una autoridad de certificación que omite publicar la revocación de un certificado después de haber sido notificada adecuadamente y en propia forma por el titular del certificado ¿debe poder excluir contractualmente su responsabilidad por daños causados al titular del certificado cuando éste es utilizado por un tercero?

En relación a la responsabilidad extracontractual, tanto respecto de la autoridad de certificación y las terceras partes que confían en los certifi-

cados, como entre los titulares de certificados y dicha partes, la Comunicación guarda silencio. Parece apropiado para cualquier régimen que gobierne las autoridades de certificación tratar esta materia y establecer un régimen de responsabilidad que cree un equilibrio adecuado entre los actores anteriormente mencionados.

La aplicación ordinaria de las reglas de responsabilidad extracontractual da lugar a que la persona que sufre un daño en relación a un certificado tenga la carga de demostrar la falta de diligencia de la autoridad de certificación. Sin embargo, dada que la materia relacionada con la emisión y mantenimiento de certificados tiene un contenido tecnológico muy importante, esta carga de la prueba puede devenir sumamente difícil de conseguir. En consecuencia, una solución que establezca la inversión de la carga de la prueba podría ser conveniente (10). A través de este enfoque, la autoridad de certificación tendría la carga de probar que actuó diligentemente. Quizás esta inversión de la carga de la prueba sería también apropiada en el contexto de contratos entre la autoridad de certificación y los titulares de certificados.

Es probable que este enfoque sea adoptado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/UNCITRAL) en un nuevo modelo de ley sobre firmas digitales, autoridades de certificación que complementa a la Ley Modelo sobre Comercio Electrónico de 14 de Junio de 1996 (11). El proyecto de ley de UNCITRAL también propone una presunción de responsabilidad que puede ser rebatida por la autoridad de certificación si ésta logra demostrar que ha cumplido ciertos requisitos (por ejemplo, demostrando que actuó con diligencia en la averiguación de la identidad del titular del certificado).

La Ley de firma digital alemana no estipula ninguna regla especial en responsabilidad (12). Por el contrario, el Cuestionario público del Reino Unido sobre propuestas legislativas titulado "Sobre la provisión de licencias a terceros de confianza para llevar a cabo servicios criptográficos" propone que las autoridades de certificación deberían estar sujetas a responsabilidad objetiva atenuada por la fijación de unos límites máximos de indemnización (13).

Debe mencionarse una cuestión específica en relación a la obligación del titular de un certificado: la obligación de mantener la clave privada en

(10) POULET, Y. y JULIA BARCELÓ, R., "Health Telematics Networks: Reflections on Legislative and Contractual Models Providing Security Solutions", en *The EDI Law Review*, núm. 4, págs. 177-203.

(11) Ver (A/CN.9/437), (A/CN.9/446), (A/CN.9/WG.IV/WP.71), (A/CN.9/WG.IV/WP.73). Para un comentario sobre este proyecto de ley, ver: MADRID PARRA, A., "Firmas digitales y entidades de certificación a examen en la CNDMI/UNCITRAL", en *Actualidad Informática Aranzadi*, núm. 24, 1997, págs. 1-7.

(12) En la discusión legislativa sobre la Ley de firma digital, se decidió, que debido a la novedad del problema de la responsabilidad, abtenerse de incluir cualquier provisión especial en responsabilidad y en su lugar analizar si en el futuro sería adecuado incluir alguna regla especial en responsabilidad.

(13) Ver sección V, parágrafo 43 del cuestionario (mayo 1997). Para un comentario sobre el mismo, ver: REED, C. y AVELLÁN, J., "The United Kingdom Policy on Trusted Third Parties and its Implications for EDI", en *The EDI Law Review*, núm. 3, 1997, págs. 81-89.

secreto, así como la de notificar inmediatamente a la autoridad de certificación si la clave ha sido puesta en peligro de alguna manera. A pesar de que algunos autores han criticado que el titular de un certificado soporte el riesgo hasta que haya notificado el compromiso de la clave (14), en principio, parece que este es el único método factible de repartir el riesgo. Sería inapropiado imponer cualquier tipo de responsabilidad sobre la autoridad de certificación hasta que ésta haya recibido notificación, ello al margen de que las autoridades de certificación eduquen a los titulares de certificados sobre la importancia de guardar cuidadosamente la clave privada y el certificado. Además, algunas medidas técnicas, tales como las tarjetas inteligentes utilizadas juntamente a mecanismos biométricos, podrían reducir los riesgos asociados con la pérdida y robo de la clave privada y del certificado.

III. Reconocimiento legal de las firmas digitales

Las firmas digitales no pueden jugar su papel en la facilitación del comercio electrónicos a menos que sean reconocidas legalmente. En otras palabras, las firmas digitales deben ser legalmente equivalentes a las firmas manuscritas antes de que puedan convertirse en una herramienta efectiva del comercio.

Desgraciadamente, como muy bien señala la Comisión en su Comunicación, por el momento no se concede a las firmas digitales un reconocimiento legal adecuado. En la actualidad, las leyes de los Estados Miembros imponen requisitos de firma manuscrita y de escrito como condición de validez contractual, de eficacia y como condición de su admisión y valoración como prueba (15). Estos requisitos varían de un Estado Miembro a otro, tanto en sus términos como en sus motivos.

En algunos sistemas legales, en materia de contratos, es frecuente encontrar el requisito de forma escrita y firma manuscrita. En estos sistemas, por ejemplo, algunos tipos de contratos son inválidos o ineficaces a menos que estén documentados por escrito y acompañados por una firma manuscrita, a menudo por motivos de protección del consumidor (16). En otros casos, la prueba documental consistente en un escrito con una firma manuscrita tiene mayor peso probatorio que otros medios de prueba (17), y es dudoso si las firmas digitales serán capaces de gozar del mismo tra-

(14) Wright, B., "Eggs in Baskets: Distributing the Risks of Electronic Signatures", en *The John Marshall Journal of Computer & Information Law*, vol. XV, núm. 2, págs. 189-201.

(15) Ver Lamberterie, I., "La valeur probatorie des documents informatiques dans les pays de la CEE", en *Revue International de Droit Comparé*, núm. 3, 1992.

(16) Por ejemplo, el artículo 1341 del Código civil belga y del Código civil francés contienen requisitos de firma cuando el valor del objeto del contrato (por ejemplo un contrato de compraventa) sea superior a una cantidad determinada.

(17) Este es el caso del sistema alemán. Para un comentario en esta cuestión, véase: Blechschmidt, R., "The German Basic Electronic Data Interchange Model Agreement Versus the European Model EDI Agreement: Some Reflections on German Law", en *The EDI Law Review*, núm. 3, 1996, págs. 107-124. Para un comentario más general, ver: Rihaczek, K., "Digital Signature Surrogates for Open EDI", en *The EDI Law Review*, núm. 2, 1995, págs. 229-240.

tamiento. Es más, incluso en aquellos países en los cuales no se da a la prueba documental un peso específico, los Tribunales no siempre están dispuestos a conceder a los documentos electrónicos acompañados de firmas digitales el mismo valor probatorio que a sus homólogos acompañados por firmas manuscritas.

En la medida en que las firmas digitales pueden proporcionar, cuanto menos, el mismo nivel de seguridad en relación a la autenticidad e integridad de un documento que el que pueden proporcionar las firmas manuscritas, lo anterior constituye una situación anacrónica. Como observa la Comunicación "en orden a lograr la aceptación más amplia posible de las firmas digitales, las sistemas legales nacionales necesitan adaptarse para asegurar el mismo reconocimiento y tratamiento a las firmas digitales que a las manuscritas".

Desde nuestro punto de vista, para facilitar el desarrollo del comercio electrónico, la Comisión Europea debería establecer el reconocimiento de las firmas digitales. La Comunicación parece considerar esta proposición, indicando que la Comisión pretende continuar con la opinión general que hace falta estipular el reconocimiento legal de las firmas digitales a nivel de la Comunidad Europea (18). En esta dirección, la Comisión sigue los pasos de algunas instituciones internacionales que señalaron la necesidad de otorgar reconocimiento legal a los nuevos mecanismos que autentifican los mensajes y ofrecen integridad (por ejemplo, UNCITRAL, Programa Tedis, Consejo de Europa, Grupo de Trabajo 4 de la Grupo de Trabajo para la facilitación de los procedimientos de comercio Internacional de las Comisión para Europa de las Naciones Unidas) (19).

Como indica la Comunicación, cualquier régimen legal debe ser lo suficientemente flexible para acomodar futuros desarrollos tecnológicos. El reconocimiento legal deberá reconocer el mismo tratamiento a la firma manuscrita que a la digital, pero, al mismo tiempo, ser lo suficientemente flexible y neutral como para integrar nuevos medios para autenticar y conseguir la integridad de los mensajes. En efecto, la ley no debe centrarse exclusivamente en las firmas digitales actuales, esto es, no debe prever un reconocimiento de un tipo de tecnología especial como es la actual tecnología de las firmas digitales, porque dicha tecnología podría en el futuro no ofrecer la seguridad adecuada. El progreso técnico podría dar lugar a una situación en la que las actuales formas de criptografía de clave pública dejaran de ofrecer la seguridad e integridad adecuadas (por ejemplo, porque la capacidad de computación de los ordenadores aumente hasta el punto de que sea posible descubrir rápidamente la clave privada a partir de la clave pública o bien porque ciertos algoritmos criptográficos no ofrezcan seguridad porque los problemas matemáticos de fondo sean

(18) Comunicación, Sección IV, 1.2. (ii).

(19) Para UNCITRAL, véase la Recomendación 1985 (A/40/17), así como el artículo 7 de la Ley Modelo sobre comercio electrónico de 14 de junio de 1996 (A/51/17). Para Tedis, véase, Tedis- Situation Juridique des Etats Membres au regard du transfers électronique de données, Bruxelles, Commision des Communautés Européenes. Para el Grupo de Trabajo para la Facilitación del Comercio de la Comisión para Europa de las Naciones Unidas, véanse las Recomendaciones UN/EC núm. 12, núm. 13 y núm. 14.

resueltos). Es más, una legislación que especifique una tecnología determinada puede desalentar el desarrollo de otras tecnologías.

En consecuencia, la Comisión Europea y los Estados Miembros deberían empezar inmediatamente el proceso de identificar, analizar y catalogar los diversos requisitos legales en los que las firmas digitales y los documentos electrónicos se ven perjudicados con respecto de sus equivalentes papel. A continuación se necesitará emprender la difícil tarea de concebir un nuevo y armonizado enfoque de estos requisitos que no esté formulado en la terminología del tradicional mundo de los documentos papel y que establezca adecuado reconocimiento a las firmas digitales y a sus descendientes técnicos. Este estandard debería identificar el nivel necesario de autenticidad y de integridad requerido para un particular tipo de documentos (sean tradicionales o papel) y establecer un estandard técnico neutral de acuerdo con el cual cualquier forma de conseguir el requisito de autoridad e integridad será acordado igual reconocimiento legal (20).

Una cuestión importante que se plantea en este contexto es el papel de las autoridades de certificación. Como también reconoce la Comunicación, los efectos legales de los documentos firmados digitalmente pueden estar ligados a la seguridad de las autoridades de certificación. En efecto, en la medida en que las autoridades de certificación, por ejemplo, aseguren la conexión entre la clave pública y el titular del certificado, pueden favorecer el valor y la seguridad de las firmas digitales.

Sin embargo, se plantea la cuestión de si los nuevos estándares (mencionados más arriba) que gobiernen el nivel necesario de autenticidad e integridad requerirán para todos los documentos la implicación de una autoridad de certificación. Por ejemplo, ¿debería la ley requerir, como algunos sugieren, que un documento electrónico sea considerado como un documento escrito para calificarlo como prueba documental o para otros fines sólo si está acompañado por una firma digital que ha sido reconocida por una autoridad de certificación que ha cumplido con ciertos requisitos obligatorios para el establecimiento y funcionamiento de las mismas? Desde nuestro punto de vista, esta condición parece equivocada, al menos en ciertas circunstancias. Por ejemplo, algunas compañías que lleven a cabo regularmente negocios entre ellas por vía electrónica, podrían elegir intercambiar las claves de manera privada, evitando así el gasto y la carga de utilizar una autoridad de certificación. Sería inapropiado denegar el mismo reconocimiento a los documentos firmados utilizando firmas digitales cuya clave pública ha sido reconocida de la manera que se acaba de señalar. Quizás la ley debería prever que aquellas firmas digitales certificadas por una autoridad de certificación que ha obtenido una licencia deberían ser legalmente reconocidas *prima facie*, pero debiera permitirse a aquellos que utilizan otro tipo de firmas (firmas electrónicas distintas de la firma digital o bien cualquier tipo de firma) probar su validez por medio de la demostración de la seguridad y fiabilidad del sistema de firma de que se trate.

---

(20) Un criterio funcional semejante se incorpora en el artículo 7 de la Ley Modelo sobre comercio electrónicos de UNCITRAL.

Los documentos electrónicos acompañados por firmas digitales ofrecen un nivel mas alto de autenticidad e integridad que los documentos tradicionales firmados de forma manuscrita. Por lo tanto, exigir que un documento electrónico sea acompañado de una firma digital y un certificado emitido por una autoridad de certificación licenciada para que este documento sea reconocido legalmente impondría una carga demasiado pesada para la firmas digitales, incluso más pesada que la que ha sido puesta tradicionalmente a los documentos papel. En realidad, para la mayoría de documentos electrónicos sería inoportuno imponer tal alto estandard de autenticidad e integridad.

En efecto, exigir que un documento electrónico tenga que estar acompañado por una firma digital y un certificado emitido por una autoridad de certificación sería lo mismo que requerir una firma manuscrita que esté autentificada por un notario. Si no se exige para todos los documentos la intervención del notario para que la firma sea válida o eficaz, ¿por qué debe requerirse una firma digital acompañada de un certificado emitido por una autoridad de certificación? Quizás fuese conveniente requerir un certificado sólo en los casos en los cuales fuese necesario la presencia de un notario en el contexto de documentos convencionales y cuando las comunicaciones fueran hechas con las autoridades como la Administración Tributaria y la Seguridad Social.

En cualquier caso, el enfoque tecnológico neutro que se adoptara debiera permitir a los tribunales la posibilidad de aceptar los avances tecnológicas capaces de ofrecer autenticidad e integridad. Cualquiera que sea la forma en que se formule este enfoque, deberá asegurar (al menos para el futuro próximo) que los documentos electrónicos acompañados de una firma digital y de un certificado emitido por una autoridad de certificación establecida y operando de acuerdo a ciertos estándares sean equivalentes a la firma manuscrita.

Los documentos públicos electrónicos podrían considerarse como una categoría especial y ser reconocidos solamente si vinieran acompañados de certificados emitidos por una autoridad de certificación que hubiera obtenido una licencia. A pesar de que los notarios probablemente no celebrarán dicha posibilidad, uno podría preguntarse si las autoridades de certificación tienen un papel notarial vital a cumplir en el futuro digital y si podrían suplantar gran parte del rol de los notarios en el mundo electrónico. Y si es así, ¿cómo puede asegurarse que el régimen de licencias no es usado para limitar el número de autoridades de certificación y, por tanto, para restringir la competencia entre las autoridades de certificación?

IV. Regulación de la criptología

De aquí en adelante, nos centraremos en el otro tema principal tratado por la Comunicación: la utilización de la criptografía. Tratamos este tema de forma más superficial que el tema de las firmas digitales porque ha sido de objeto de numerosos debates y comentarios.

Como la Comunicación dice, el desarrollo del comercio electrónico y de otras muchas aplicaciones de la sociedad de la información dependerá de la capacidad a bajo coste de mantener las comunicaciones electrónicas en secreto (21). La Comunicación prevé varios ejemplos en los cuales el requisito de la confidencialidad es especialmente claro: el *teleshopping* y *telebanking* (donde los consumidores deben tener la seguridad que los datos personales, tales como los números de las tarjetas de crédito que viajan en la red son guardados de manera confidencial); comunicaciones comerciales (los casos en los que las compañías quieren protegerse de espionaje industrial); aplicaciones telemáticas relativas a la salud (en las que los pacientes deben ser protegidos contra revelaciones no autorizado de historiales médicos); etc. Como se señaló más arriba, en la introducción, los sistemas de criptografía simétrica son en la actualidad la principal forma de conseguir confidencialidad de las comunicaciones.

En la actualidad existe un vivo debate sobre la regulación de la criptografía en el que la Comisión ha tomado una postura liberal con respecto a los principales aspectos de este debate. En particular, la Comunicación plantea los siguientes aspectos:

- Medidas para controlar la exportación.
- Medidas de control domésticas.
- Sistemas de *Key escrow* y *key recovery*.
- Aspectos de protección de datos.

Medidas de control de la exportación

Como apunta la Comunicación, la exportación de la criptografía ha sido objeto de restricciones para impedir que los países extranjeros pudiesen utilizar criptografía calificada como "dura", esto es, técnicamente muy difícil de desencriptar sin la aplicación de la clave. Internacionalmente, dichos controles se han impuesto a través del Arreglo de Wassenaar (22), el cual reemplazó la lista COCOM. En la Unión Europea, la exportación de ciertas tecnologías criptográficas está controlada a través de la Regulación de doble uso de Diciembre 1994 (23). Como señala la Comunicación, en la medida en que la Regulación sobre doble uso permite los controles criptográficos en el transporte de productos criptográficos de un Estado Miembro a otro, puede provocar distorsiones en el funcionamiento del Mercado Único.

(21) Comunicación, sección III.1 (iii)

(22) Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies (Dec. 19, 1995).
http://2.nttea.com:8010/infomofa/press/e-wassenaar.html:http://ideath.parrhesia.com/wassenaar/wassenaar.html

(23) Council Regulation (EC) 3381/94, 19-12-1994. Council Decision 94/942/CFSP, 19.12.94, OJ L367/78 (31.12.94), establece la lista de bienes de uso dual cobiertos por la Regulación.

En relación a las acciones legislativas que deben ser tomadas en materia de controles a la exportación, la Comunicación no sugiere ninguna acción respecto del Arreglo de Wassenaar, probablemente porque la Comisión no desea excederse demasiado en los límites de su poder respecto a materias de seguridad nacional. Sin embargo, afortunadamente, la Comunicación sugiere que la Regulación de doble uso debería ser liberalizada (24). En concreto, la Comunicación sugiere la progresiva eliminación de controles intra-comunitarios en productos criptográficos comerciales.

Medidas de control doméstico

En comparación con los controles a la exportación de productos criptográficos, los controles domésticos a la criptografía son relativamente raros. Entre los Estados Miembros de la Unión Europea, sólo Francia tiene una regulación amplia sobre la criptografía. Sin embargo, hay intensos debates en curso en diversos Estados de la Unión Europea (y Estados Unidos) sobre la posibilidad de adoptar este tipo de regulación. Como apunta la Comunicación, las autoridades policiales, así como las agencias de inteligencia de cada país, están a favor de implantar controles domésticos sobre la criptografía por el temor a que el uso generalizado de comunicación encriptadas disminuirá su capacidad para luchar contra la criminalidad y para prevenir el terrorismo.

La Comunicación apunta que los mecanismos domésticos de control propuestos podrían hacer ilegal el uso de la criptografía (o al menos de ciertos tipos de criptografía) a menos que hubieran sido autorizados. Alternativamente o adicionalmente, la exportación e importación de productos y servicios criptográficos (como aquellos que emplean criptografía dura) podrían ser sometidos a un proceso de autorización. El principal objetivo de este régimen es asegurar que la criptografía disponible a los usuarios sea relativamente débil (prácticamente inútil) o bien sometida al control de los gobiernos a través de procesos de *key escrow* o similares.

La Comunicación es directa en su juicio acerca de estos mecanismos de control doméstico. Básicamente, señala que estos mecanismos serían inútiles y contraproductivos. Que no impedirían a los criminales el uso de técnicas de criptografía pero "podrían impedir a compañías y ciudadanos su protección contra ataques criminales (25)". Es más —y ello ofrece bases importantes para iniciativas de la Comisión en esta materia— por medio del establecimiento de diferentes reglas que gobiernen el uso y la venta de técnicas criptográficas, podrían crearse obstáculos al funcionamiento del Mercando Único. Además, la formulación de leyes que regulen la criptografía tendrá un efecto directo en la intimidad y libertad de expresión y de asociación. Sólo podemos esperar que los Estados Miembros se den cuenta de la sabia política de no intervención de la Comisión respecto de una regulación de la criptografía.

(24) Comunicación, sección IV (II).
(25) Comunicación, sección III.2.1.

Sistemas de "Key escrow" y "key recovery"

Los sistemas que se han propuesto para controlar el uso de la criptografía con las actividades ilegales son *key scrow* y de *key recovery*. El sistema *key escrow* requiere que una copia de la clave privada sea depositada directamente ante las agencias de policía o bien ante los llamados "terceros de confianza" quienes, bajo ciertas circunstancias se verían obligados a revelar las claves a las agencias de inteligencia gubernamentales. En el sistema *key recovery*, la información sobre la clave es ofrecida al gobierno o al tercero de confianza lo que permitiría que las agencias de inteligencia conocer la clave si fuera necesario para desencriptar el mensaje para propósitos policiales.

La Comunicación adopta una posición negativa, que nosotros asumimos, respecto a los sistemas de *key escrow* y *key recovery*. Como la Comunicación señala (26), este sistema sería inefectivo para los fines de las agencias de policía puesto que serían fácilmente neutralizados. Al mismo tiempo, los sistemas de *key escrow* y *key recovery* disminuirían de manera significante el atractivo de los usuarios de criptografía. Obviamente, la intervención de un tercero en una comunicación confidencial incrementa su vulnerabilidad y, en consecuencia, disminuye la confianza en la confidencialidad de las comunicaciones electrónicas. Relacionado con este hecho, se plantean preocupaciones serias respecto a la protección de datos personales. Los sistemas de *key escrow* y *key recovery* impondrán costes importantes en el uso de la criptografía, especialmente cuando dichos sistemas se implanten a escala global. En resumen, las consecuencias adversas que se derivarían de la imposición de sistemas de *key escrow* y *key recovery* obstaculizarían el desarrollo del comercio electrónico sin ofrecer ningún beneficio real a las agencias de policía.

Intimidad

La Comunicación señala la importancia de la criptografía para mantener la confidencialidad de las comunicaciones. En particular, por medio del empleo de métodos criptográficos los responsables del tratamiento de los ficheros pueden cumplir las obligaciones impuestas por la Directiva de protección de datos personales.

La Comunicación da a entender que la Comisión podría utilizar la Directiva de protección de datos y el poder de la Comisión para ir contra ciertas leyes que obstaculizan el uso de la criptografía. Como la Comunicación señala, el libre flujo de datos personales a través del Mercado Interno depende de la posibilidad de los métodos criptográficos de "viajar" con la información personal. Por tanto, las leyes que regulan la criptografía de los Estados Miembros no deben ser distintas, porque de lo contrario se crearían obstáculos para el flujo de información y, en con-

(26) Comunicación, sección III.2.3

secuencia se producirían restricciones en el flujo de bienes y servicios entre los Estados Miembros. En palabras de la Comunicación: "[c]ualquier regulación que obstaculice el uso de los productos y servicios criptográficos en el interior el Mercado Interno consecuentemente obstaculiza el flujo seguro y libre de información personal y la disposición sobre bienes y servicios afines" (27).

Tendencias legislativas de la Comisión

Al establecer los criterios sobre criptografía, la Comisión que, por un lado, reconoce la competencia de los Estados Miembros en relación a la materia de seguridad nacional y de policía, señala que debe actuar contra la regulación sobre la criptografía que infrinja la ley comunitaria, por ejemplo la ley sobre libre movimiento de bienes y servicios, así como las leyes de protección de datos personales. En relación a ello, la Comunicación señala que los Estados Miembros están obligados a notificar a la Comisión de nuevas leyes nacionales que podrían crear obstáculos al mercado interno, e indica que dichas notificaciones podrían poner las bases para una acción de la Comisión en esta materia (28).

Estas orientaciones legislativas deben ser bienvenidas. Sin duda, la Comisión tiene razón en apuntar que no habrá mercado interno para el comercio electrónico sin un mercado interno para la criptografía. Es vital para evitar inconsistencias internas la armonización de los reglas de los Estados Miembros en criptografía y la Comisión tiene un rol esencial en la consecución de este objetivo.

Además, la tendencia internacional de la Comunicación es importante. Tal y como ésta indica, la naturaleza global del comercio electrónico requerirá que la Comunidad Europea persiga un marco internacional compatible para las firmas digitales y criptografía, incluyendo el establecimiento de stándares técnicos necesarios para la interoperabilidad y el reconocimiento de certificados en una base internacional. Esperamos que la Comisión promoverá su regulación de la criptografía con sus socios principales así como con las organizaciones internacionales como la WTO y OCDE.

En lo que concierne a su programa futuro, la Comisión pretende organizar una reunión internacional sobre las cuestiones tratadas por la Comunicación durante el primer cuatrimestre de 1998 y hacer una propuesta para más acciones (quizás incluyendo una directiva en firmas digitales) durante el segundo cuatrimestre de 1998. Finalmente, la Comunicación se fija como objetivo haber logrado el establecimiento de un marco legal europeo legal común sobre criptografía antes del año 2000.

(27) Comunicación, sección III.2.4., sección III.3 (v)

(28) En relación a este aspecto, es importante señalar que el gobierno francés ha notificado a la Comisión sobre las propuestas legislativas sobre criptografía.

V. Conclusión

Un aire refrescante sopla desde Bruselas. Por primera vez desde que el debate sobre criptografía comenzó, una comunicación oficial ha admitido claramente la necesidad del reconocimiento legal de las firmas digitales en una escala global y la eliminación de los obstáculos a la disponibilidad para el público en general de la criptografía dura. La asunción rápida de estos objetivos legislativos establecidos por la Comunicación establecería una de las principales condiciones para el crecimiento del comercio electrónico y el desarrollo de la Sociedad de la Información en Europa.